Report: VLAN-Based Secure Network Design with Guest Isolation

Abstract

This project demonstrates the design and implementation of a secure enterprise-style network in Cisco Packet Tracer. The network integrates multiple VLANs for departmental separation, inter-VLAN routing using a router-on-a-stick configuration, DHCP services for dynamic addressing, and ACLs for traffic control. Wireless access points were deployed for HR, IT, and Guest VLANs, extending mobility without sacrificing security. Testing verified that departmental communication, internet access, and guest isolation policies function as intended.

Introduction

The purpose of this project was to design and configure a medium-scale enterprise network that meets the following goals:

1. Logical separation of departments through VLANs.
2. Secure inter-VLAN communication using router sub-interfaces.
3. DHCP services for simplified IP address assignment.
4. Guest VLAN isolation with ACLs — guests can communicate with each other and access the internet, but not HR or IT resources.
5. Integration of wireless access to VLANs without breaking security policies.

This design mirrors real-world enterprise requirements, such as separating business-critical departments from guest traffic while still providing internet access.

Design

Scope:

- Departments: HR, IT, Guest.
- Devices: One Router, one Switch (2960), Access Points, PCs, and Wireless Devices.
- Services: DHCP, SSH management, ACLs.

Requirements:

- VLANs: HR (10), IT (20), Guest (30).

- IP Addressing:
    - HR: 192.168.10.0/24
    - IT: 192.168.20.0/24
    - Guest: 192.168.30.0/24
- Each VLAN must have DHCP-provided addresses.
- Guest VLAN must be fully isolated from HR and IT.
- Wireless devices must connect via SSID and integrate into their respective VLANs.

Limitations:

- Packet Tracer does not fully simulate wireless security protocols (e.g., WPA2 Enterprise), so basic WPA2-PSK was used.
- Internet simulation was approximated using a DNS server rather than a true WAN.

Development

Network Solution

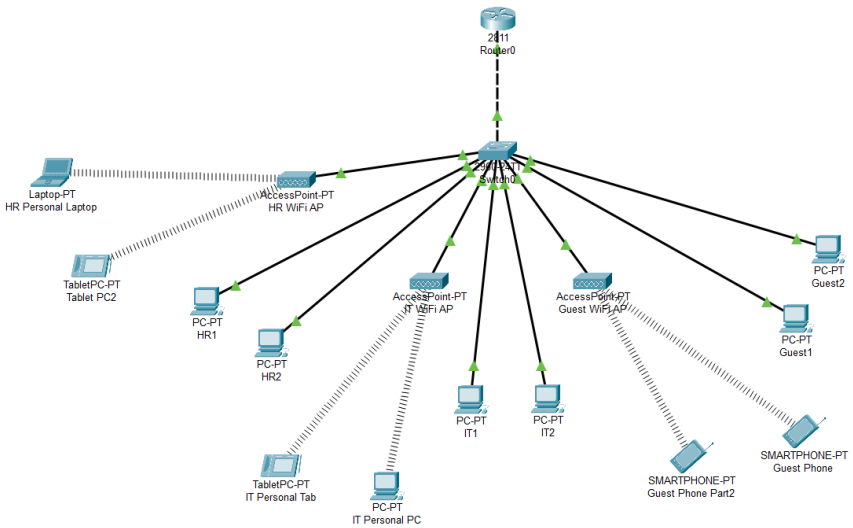
1. **VLANs on the Switch**
    - VLAN 10 (HR), VLAN 20 (IT), VLAN 30 (Guest) created.
    - Access ports assigned to PCs.
    - Trunk configured on Switch Fa0/1 → Router Fa0/1.
2. **Router-on-a-Stick**
    - Sub-interfaces Fa0/1.10, Fa0/1.20, Fa0/1.30 configured with encapsulation dot1Q and IP addresses.
    - DHCP pools created for each VLAN with exclusions for gateway addresses.
3. **ACLs for Guest Isolation**
    - Extended ACL applied inbound on Guest sub-interface:
    - deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
    - deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    - permit ip 192.168.30.0 0.0.0.255 192.168.30.0 0.0.0.255
    - permit ip any any

- This ensures Guest → HR/IT blocked, Guest ↔ Guest allowed, Guest → Internet allowed.

4. **Wireless Access**
   - Separate Access Points deployed for HR, IT, and Guest VLANs.
   - Each AP assigned SSID + WPA2-PSK and connected via Ethernet to access ports mapped to VLANs.
   - Wireless laptops and tablets connected successfully and received DHCP addresses.

Network Description

- **Diagram:**



- **Functional Blocks:**
  - HR VLAN → Router sub-interface Fa0/1.10 → Internet/DNS.
  - IT VLAN → Router sub-interface Fa0/1.20 → Internet/DNS.
  - Guest VLAN → Router sub-interface Fa0/1.30 → ACL filter → Internet/DNS.
- **Data Paths:**
  - Inter-VLAN traffic flows through router sub-interfaces.
  - Guest VLAN traffic filtered by ACL before routing decisions.
- **VoIP (if included):** Voice VLANs can be assigned similarly with switchport voice VLAN on access ports.

Testing and Results

Testing Steps:

1. Ping between HR1 ↔ IT1 → **successful** (inter-VLAN works).
2. Ping from Guest1 → HR1 → **denied**, ACL counters increased.
3. Ping from Guest1 → Guest2 → **successful**, ACL counters increased on "permit guest↔guest" line.
4. DHCP: All PCs and wireless clients successfully obtained IPs from router pools.
5. SSH: Secure management enabled via crypto key generate rsa and line vty config.
6. Wireless: HR and IT laptops connected to their SSIDs and received IPs in the correct VLANs.

Screenshots:

```
RouterinUse#show ip interface brie
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    down
FastEthernet0/0.10     unassigned      YES unset  up                    down
FastEthernet0/0.20     unassigned      YES unset  up                    down
FastEthernet0/0.30     unassigned      YES unset  up                    down
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/1.10     192.168.10.1    YES manual up                    up
FastEthernet0/1.20     192.168.20.1    YES manual up                    up
FastEthernet0/1.30     192.168.30.1    YES manual up                    up
Vlan1                  192.168.1.1     YES manual up                    down
```

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   HR                               active    Fa0/2, Fa0/3, Fa0/8
20   IT                               active    Fa0/4, Fa0/5, Fa0/9
30   Guest                            active    Fa0/6, Fa0/7, Fa0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
RouterinUse#show access-lists GUEST_RESTRICT
Extended IP access list GUEST_RESTRICT
    deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (4 match(es))
    deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    permit ip 192.168.30.0 0.0.0.255 192.168.30.0 0.0.0.255
    permit ip any any
```

```
C:\>ping 192.168.20.104

Pinging 192.168.20.104 with 32 bytes of data:

Reply from 192.168.20.104: bytes=32 time=28ms TTL=127
Reply from 192.168.20.104: bytes=32 time=30ms TTL=127
Reply from 192.168.20.104: bytes=32 time=31ms TTL=127
Reply from 192.168.20.104: bytes=32 time=16ms TTL=127

Ping statistics for 192.168.20.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 31ms, Average = 26ms
```

```
C:\>ping 192.168.30.102

Pinging 192.168.30.102 with 32 bytes of data:

Reply from 192.168.30.102: bytes=32 time=27ms TTL=128
Reply from 192.168.30.102: bytes=32 time=32ms TTL=128
Reply from 192.168.30.102: bytes=32 time=35ms TTL=128
Reply from 192.168.30.102: bytes=32 time=34ms TTL=128

Ping statistics for 192.168.30.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 35ms, Average = 32ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

IT Device unreachable by guest devices. 1

Conclusions

This project demonstrated how to design and configure a secure multi-VLAN enterprise network in Packet Tracer. Key lessons learned include:

- VLANs effectively segment departmental traffic.
- Router-on-a-stick provides inter-VLAN routing with minimal hardware.
- ACLs are order-sensitive; deny rules must precede permit rules.
- Wireless access can be extended into VLANs by mapping SSIDs to VLANs via access points.
- Testing with show access-lists provides verification of security policies.

This design reflects real-world practices for balancing connectivity, security, and scalability.